The International Journal Of Engineering And Science (IJES)
||Volume|| 2 ||Issue|| 10 ||Pages|| 23-31 ||2013||
ISSN (e): 2319 – 1813 ISSN (p): 2319 – 1805

Wireless Network Management

[1] Ebole Alpha .F.
[1] *Department of Computer Science Babcock University*

ABSTRACT

The vast proliferation in the number and type of mobile and wireless Network devices along with their widespread use has been the emerging trend that dominated next-generation mobile and wireless Network. Such an environment raises an unprecedented demand for the dynamic, lightweight management of the multitude of mobile and wireless devices, to ease the complexity of their administration and optimise the overall system performance. Focusing on the overall network management aspects, a key issue is the efficient management of the system resources, spanning from the physical layer, to the protocol stacks and up to the application and services layer. To this end, the notions of configurability and autonomic networking provide a solution to this problem, fostering the introduction of intelligence in mobile, wireless devices and network nodes .This article investigates this challenge, by addressing the dynamic planning, organizing, implementation and control towards the management of wireless network as well as its nodes

Wireless Networks (WNs) have become an emerging new research area in the distributed and Heterogeneous computing environment. It plays an important role in the pervasive computing to support a wide range of applications of our daily life in future. More specifically, such wireless network proposes a new monitoring and control model for applications to operate as environmental monitoring, public safety, medical, transportation and military. Most of those applications share similar features such as difficult to access because of geographical locations where the network has been deployed, the large scale of deployment, high mobility, and prone to failure. Accordingly, the traditional network maintenance and management approaches become impractical under such very dynamic conditions. Furthermore, network management becomes extremely important and vital in order to keep the whole network and application work properly. Until now, there still doesn't emerge a considerable network management solution for WN. Most of existing research addresses one or several application-specific problems in WNs, instead of considering from network management aspects. These paper overviews several related on-going research approaches, and provides discussion and provision of some design issues and requirements for building efficient management architecture for WN.

Date of Submission: 10th, October, 2013 ⟺ Date of Acceptance: 30th, October, 2013

I. INTRODUCTION

Until recently, acceptance of Wireless Networks and mobile devices have been slow due tomany factors including but not limited to lack of standardization, slow data speeds and high costs. Recent market developments, however, have led to rapid market growth. The IEEE 802.11b standard, which was introduced in 1999, now enables wireless Network to reach data rates up to 11 Mb/s. Demand for wireless Network has also been fuelled by growth in mobile computing devices such as laptops and personal digital assistants (PDAs), reduced prices and increased demand for Internet access anywhere/anytime.

Wireless Network applications include Internet access, supply chain management and customer relationship management, to name a few. Traditionally, wireless Network was used primarily in an area such as education, finance, healthcare, manufacturing, and retail. More recently, however, wireless Network has appealed to enterprise customers and public access areas such as airports, convention centres and hotels. Wireless Network are attractive to enterprise customers who manage large numbers of network adds, moves and changes for their transient employees, such as call centers, hot-desk environments for satellite offices and ad-hoc groupings of employees for meetings or training.

Even though wireless networks introduce a new, flexible way of working, they
present new challenges as well. Security management, data throughput maintenance, hardware interoperability and problem isolation can easily affect the overall satisfaction of wireless Network customers. Moreover, network managers expect wireless Network to have the same level of security, manageability and scalability as their wired Networks.

A wireless network management tool is a valuable solution for network managers deploying wireless networks because a wireless protocol analyzer, that can observe each of the layers of the stack, quickly reveals problems that other tools can easily miss. The short-term benefit of this tool is immediate reduction of the amount of time spent in troubleshooting or pinpointing whether the issue is wired or wireless in nature. The long-term benefit is that many of the network management tools provide immediate security and intrusion detection, such as identifying a rogue access point or transitive trust attacks

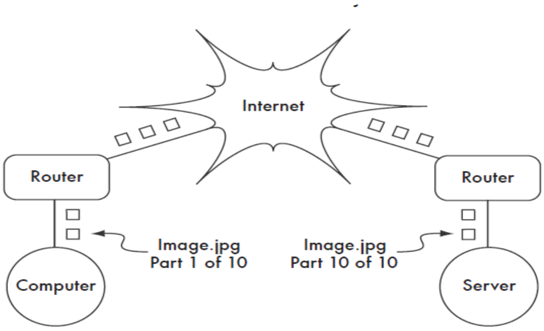
While work still needs to be done to efficiently manage wireless networks, there are a few vendors currently shipping network management tools which have gained significant momentum in usability, performance, interoperability and manageability. These vendors include Sniffer Technologies, Cisco Systems, Symbol Technologies, Lucent Technologies, Wild Packets Inc., Wireless Valley Communications and 3Com, just to mention a far.

II. LITERATURE SURVEY NETWORK DESIGN

Before purchasing equipment or deciding on a hardware platform, you should have a clear idea of the nature of plan for your communications problem. The organization in terms of network design you choose to implement in order to fit the communications problem you are trying to solve. Do you need to connect a remote site to an Internet connection in the center of your campus? Will your network likely grow to include several remote sites? Will most of your network components be installed in fixed locations, or will your network expand to include hundreds of roaming laptops and other devices?

I will begin with a review of the networking concepts that define TCP/IP, the primary family of networking protocols currently used on the Internet.

TCP/IPis also called the ***Internet protocol suite***, and it operates at layers three and four of the TCP/IP model.It is also refer to the suite of protocols that allow conversations to happen on the global Internet. By understanding TCP/IP, you can build networks that will scale to virtually any size, and will ultimately become part of the global Internet. TCP/IP networking (including addressing, routing, switches, firewalls, and routers).



This is very similar to how Internet routing works. A message is split up into many individual **packets**, and are labelled with their source and destination. The computer then sends these packets to r**outer**, which decides where to send them next. The router needs only to keep track of a handful of routes (for example, how to get to the local network, the best route to a few other local networks, and one route to a gateway to the rest of the Internet). This list of possible routes is called the **routing table**. As packets arrive at the router, the destination address is examined and compared against its internal routing table. If the router has no explicit route to the destination in question, it sends the packet to the closest match it can find, which is often its own Internet gateway (via the **default route**). And the next router does the same, and so forth, until the packet eventually arrives at its destination.

Packages can only make their way through the international postal system because we have established a standardized addressing scheme for packages. For example, the destination address must be written legibly on the front of the package, and include all critical information (such as the recipient's name, street address, city, country, and postal code). Without this information, packagesare either returned to the sender or are lost in the system. Packets can only flow through the global Internet because we have agreed on a common addressing scheme and protocol for forwarding packets. These standard communication protocols make it possible to exchange information on a global scale.

IP Addressing

In an IPv4 network, the address is a 32-bit number, normally written as four 8-bit numbers expressed in decimal form and separated by periods. Examples of IP addresses are 10.0.17.1, 192.168.1.1, or 172.16.5.23.If you enumerated every possible IP address, they would range from 0.0.0.0 to 255.255.255.255. This yields a total of more than four billion possible IP addresses (255 x 255 x 255 x 255 = 4,228,250,625); although many of these are reserved for special purposes and should not be assigned to hosts. Each of the usable IP addresses is a unique identifier that distinguishes one network node from another. Interconnected networks must agree on an IP addressing plan. IP addresses must be unique and generally cannot be used in different places on the Internet at the same time; otherwise, routers would not know how best to route packets to them.

IP addresses are allocated by a central numbering authority that provides a consistent and coherent numbering method. This ensures that duplicate addresses are not used by different networks. The authority assigns large blocks of consecutive addresses to smaller authorities, who in turn assign smaller consecutive blocks within these ranges to other authorities, or to their customers. These groups of addresses are called sub-networks, or ***subnets*** for short. Large subnets can be further subdivided into smaller subnets and a group of related addresses is referred to as an **address space**.

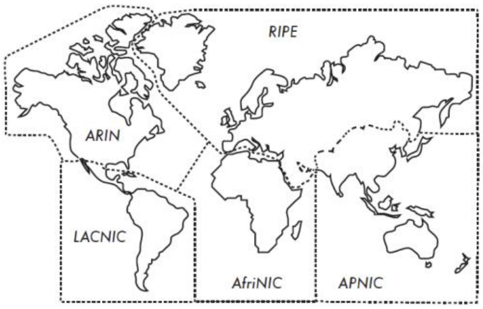
Subnets

By applying a **subnet mask**(also called a **network mask**, or simply **netmask**) to an IP address, you can logically define both a host and the network to which it belongs. Traditionally, subnet masks are expressed using dotted decimal form, much like an IP address. For example, 255.255.255.0 is one Common netmask. You will find this notation used when configuring network interfaces, creating routes, etc. However, subnet masks are more succinctly expressed using **CIDRnotation**, which simply enumerates the number of bits in the mask after a forward slash (/). Thus, 255.255.255.0 can be simplified as /24. CIDR is short for **Classless Inter-Domain Routing**, and is definein RFC15181.

A subnet mask determines the size of a given network. Using a /24 netmask, 8 bits are reserved for hosts (32 bits total - 24 bits of netmask = 8 bits for hosts). This yields up to 256 possible host addresses (2 = 256). By convention, the first value is taken as the **network address**(.0 or 00000000), and the last value is taken as the **broadcast address**(.255 or 11111111). This leaves 254 addresses available for hosts on this network.

Global IP Addresses

Have you ever wondered who controls the allocation of IP space? ***Globally*** **routable IP addresses**are assigned and distributed by **Regional InternetRegistrars**(**RIR**s) to ISPs. The ISP then allocates smaller IP blocks to theirclients as required. Virtually all Internet users obtain their IP addressesfrom an ISP.The 4 billion available IP addresses are administered by the **InternetAssigned Numbers Authority**(**IANA**). IANA has dividedthis space into large subnets, usually /8 subnets with 16 million addresseach. These subnets are delegated to one of the five regional Internet registries(RIRs), which are given authority over large geographic areas.



Authority for Internet IP address assignments is delegated to the five Regional Internet Registrars.

The five RIRs are:
- African Network Information Centre (AfriNIC, *http://www.afrinic.net/*)
- Asia Pacific Network Information Centre (APNIC, *http://www.apnic.net/*)
- American Registry for Internet Numbers (ARIN, *http://www.arin.net/*)
- Regional Latin-American and Caribbean IP Address Registry (LACNIC, *http://www.lacnic.net/*)
- Réseaux IP Européens (RIPE NCC, *http://www.ripe.net/*)

Your ISP will assign globally routable IP address space to you from the pool allocated to it by your RIR. The registry system assures that IP addresses are not reused in any part of the network anywhere in the world. Once IP address assignments have been agreed upon, it is possible to pass packets between networks and participate in the global Internet. The process of moving packets between networks is called ***routing***.

Static IP Addresses

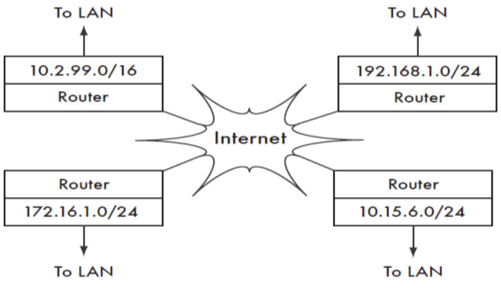
A static IP address is an address assignment that never changes. Static IP addresses are important because servers using these addresses may have DNS mappings pointed towards them, and typically serve information to other machines (such as email services, web servers, etc.). Blocks of static IP addresses may be assigned by your ISP, either by request or automatically depending on your means of connection to the Internet.

Dynamic IP Addresses

Dynamic IP addresses are assigned by an ISP for non-permanent nodes connecting to the Internet, such as a home computer which is on a dial-up connection. Dynamic IP addresses can be assigned automatically using the **DynamicHost Configuration Protocol** (**DHCP**), or the **Point-to-PointProtocol** (**PPP**), depending on the type of Internet connection. A node using DHCP first requests an IP address assignment from the network, and automatically configures its network interface. IP addresses can be assigned randomly from a pool by your ISP, or might be assigned according to a policy. IP addresses assigned by DHCP are valid for a specified time (called the ***leasetime***). The node must renew the DHCP lease before the lease time expires. Upon renewal, the node may receive the same IP address or a different one from the pool of available addresses.

Private IP addresses

Most private networks do not require the allocation of globally routable, public IP addresses for every computer in the organization. In particular, computers which are not public servers do not need to be addressable from the public Internet. Organizations typically use IP addresses from the **private addressspace** for machines on the internal network. There are currently three blocks of private address space reserved by IANA: 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16. These are defined in RFC1918. These addresses are not intended to be routed on the Internet, and are typically unique only within an organization or group of organizations which choose to follow the same numbering scheme.



: RFC1918 private addresses may be used within an organization, and are not routed on the global Internet.

If you ever intend to link together private networks that use RFC1918 address space, be sure to use unique addresses throughout all of the networks.

III. RESEARCH ELABORATION

Wireless networks

Before packets can be forwarded and routed to the Internet, layers one (the physical) and two (the data link) need to be connected. Without link local connectivity, network nodes cannot talk to each other and route packets.

To provide physical connectivity, wireless network devices must operate in the same part of the radio spectrum, this means that 802.11a radios will talk to 802.11a radios at around 5 GHz, and 802.11b/g radios will talk to other 802.11b/g radios at around 2.4 GHz. But an 802.11a device cannot interoperate with an 802.11b/g device, since they use completely different parts of the electromagnetic spectrum.

More specifically, wireless cards must agree on a common channel. If one 802.11b radio card is set to channel 2 while another is set to channel 11, then the radios cannot communicate with each other.

When two wireless cards are configured to use the same protocol on the same radio channel, then they are ready to negotiate data link layer connectivity. Each 802.11a/b/g device can operate in one of four possible modes:

1. **Master mode**(also called **AP** or **infrastructure mode**) is used to create a service that looks like a traditional access point. The wireless card creates a network with a specified name (called the **SSID**) and channel, and offers network services on it. While in master mode, wireless cards manage all communications related to the network (authenticating wire- less clients, handling channel contention, repeating packets, etc.) Wireless cards in master mode can only communicate with cards that are associated with it in managed mode.
2. **Managed mode**is sometimes also referred to as ***client*** mode. Wireless cards in managed mode will join a network created by a master, and will automatically change their channel to match it. They then present any necessary credentials to the master, and if those credentials are accepted, they are said to be ***associated*** with the master. Managed mode cards do not communicate with each other directly, and will only communicate with an associated master.
3. **Ad-hoc mode**creates a multipoint-to-multipoint network where there is no single master node or AP. In ad-hoc mode, each wireless card communicates directly with its neighbors. Nodes must be in range of each other to communicate, and must agree on a network name and channel.
4. **Monitor mode**is used by some tools to passively listen to all radio traffic on a given channel. When in monitor mode, wireless cards transmit no data. This is useful for analyzing problems on a wireless link or observing spectrum usage in the local area. Monitor mode is not used for normal communications.

APs, Clints, and Ad-Hoc nodes.

When implementing a point-to-point or point-to-multipoint link, one radio will typically operate in master mode, while the other(s) operate in managed mode. In a multipoint-to-multipoint mesh, the radios all operate in ad-hoc mode so that they can communicate with each other directly. It is important to keep these modes in mind when designing your network layout. Remember that managed mode clients cannot communicate with each other directly, so it is likely that you will want to run a high repeater site in master or ad-hoc mode. As we will see later in this chapter, ad-hoc is more flexible but has a number of performance issues as compared to using the master / managed modes.

Choosing wireless components

Unfortunately, in a world of competitive hardware manufacturers and limited budgets, the price tag is the single factor that usually receives the most attention. The old saying that "you get what you pay for" often holds true when buying high tech equipment, but should not be considered an absolute truth. While the price tag is an important part of any purchasing decision, it is vital to understand precisely what you get for your money so you can make a choice that fits your needs.

When comparing wireless equipment for use in your network, be sure to consider these variables:

- **Interoperability.** Will the equipment you are considering work with equipment from other manufacturers? If not, is this an important factor for this segment of your network? If the gear in question supports an open protocol (such as 802.11b/g), then it will likely interoperate with equipment from other sources.

- **Range.** Range is not something inherent in a particular piece of equipment. A device's range depends on the antenna connected to it, the surrounding terrain, the characteristics of the device at the other end of the link, and other factors. Rather than relying on a semifictional "range" rating supplied by the manufacturer, it is more useful to know the **transmission power**of the radio as well as the **antenna gain**(if an antenna is included).

- **Radio sensitivity.** How sensitive is the radio device at a given bit rate? The manufacturer should supply this information, at least at the fastest and slowest speeds. This can be used as a measure of the quality of the hardware, as well as allow you to complete a link budget calculation

- **Throughput.** Manufacturers consistently list the highest possible bit rate as the "speed" of their equipment. Keep in mind that the radio symbol rate (eg. 54Mbps) is never the actual throughput rating of the device (eg. About 22 Mbps for 802.11g). If throughput rate information is not available for the device you are evaluating, a good rule of thumb is to divide the device "speed" by two, and subtract 20% or so. When in doubt, perform throughput testing on an evaluation unit before committing to purchasing a large amount of equipment that has no official throughput rating.

- **Required accessories.** To keep the initial price tag low, vendors often leave out accessories that are required for normal use. Does the price tag include all power adapters? (DC supplies are typically included; power over Ethernet injectors typically are not. Double-check input voltages as well, as equipment is often provided with a US-centric power supply). What about pigtails, adapters, cables, antennas, and radio cards? If you intend to use it outdoors, does the device include a weatherproof case?

- **Availability.** Will you be able to easily replace failed components? Can you order the part in large quantity; should your project require it? What is the projected life span of this particular product, both in terms of useful running time in-the-field and likely availability from the vendor.

- **Other factors.** Be sure that other needed features are provided for to meet your particular needs. For example, does the device include an external antenna connector? If so, what type is it? Are there user or throughput limits imposed by software, and if so, what is the cost to increase these limits? What is the physical form factor of the device? How much power does it consume? Does it support POE as a power source? Does the device provide encryption, NAT, bandwidth monitoring tools, or other features critical to the intended network design.

By answering these questions first, you will be able to make intelligent buying decisions when it comes time to choose networking hardware. It is unlikely that you will be able to answer every possible question before buying gear, but if you prioritize the questions and press the vendor to answer them before committing to a purchase, you will make the best use of your budget and build a network of components that are well suited to your needs.

IV. SECURITY AND FRAUD DETECTION IN MOBILE AND WIRELESS NETWORKS

The fusion of computer and telecommunication technologies has heralded the age of information superhighway over wireline and wireless networks. Mobile cellular communication systems and wireless networking technologies are growing at an ever-faster rate, and this is likely to continue in the foreseeable future. Wireless technology is presently being used to link portable computer equipment to corporate distributed computing and other sources of necessary information. Wide-area cellular systems and wireless LANs promise to make integrated networks a reality and provide fully distributed and ubiquitous mobile communications, thus bringing an end to the tyranny of geography. Higher reliability, better coverage and services, higher capacity, mobility management, power and complexity for channel acquisition, handover decisions, security management, and wireless multimedia are all parts of the potpourri.

Further increases in network security are necessary before the promise of mobile telecommunication can be fulfilled. Safety and security management against fraud, intrusions, and cloned mobile phones, just to mention a few, will be one of the major issues in the next wireless and mobile generations. A “safe” system provides protection against errors of trusted users, whereas a “secure” system protects against errors introduced by impostors and untrusted users . Therefore, rather than ignoring the security concerns of potential users, merchants, and telecommunication companies need to acknowledge these concerns and deal with them in a straightforward manner. Indeed, in order to convince the public to use mobile and wireless technology in the next and future generations of wireless systems, telecom companies and all organizations will need to explain how they have addressed the security of their mobile/wireless systems. Manufacturers, M-business, service providers, and entrepreneurs who can visualize this monumental change and effectively leverage their experiences on both wireless and Internet will stand to benefit from it.

Concerns about network security in general (mobile and wired) are growing, and so is research to match these growing concerns. many intrusion-detection prototypes, for instance, have been created. Intrusion detection systems aim at detecting attacks against computer systems and wired net works, or against information systems in general. However, intrusion detection in mobile telecommunication networks has received very little attention. It is our belief that this issue will play a major role in future generations of wireless systems. Several telecom carriers are already complaining about the loss due to impostors and malicious intruders.

V. NETWORK SECURITY PROBLEMS

Security is an essential part of wired and wireless network communications. Interestingly enough, these systems are designed to provide open access across vast networked environments. Today’s technologies are usually network-operation-intrusive, i.e., they often limit the connectivity and inhibit easier access to data and services. With the increasing popularity of wireless networks, the security issue for mobile users could be even more serious than we expect. The traditional analogue cellular phones are very insecure. The 32-bit serial number, the 34-bit phone number, and the conversation in a cell can be scanned easily by an all-band receiver. The widely used advanced mobile phone system (AMPS) is an analogue phone system. Therefore, sending a password or a host name through this system can be a serious security issue. Other security issues in wireless networks that have been studied extensively are anonymity and location privacy in mobile networks; these have received a great deal of interest recently. A typical situation is one in which a mobile user registered in a certain home domain requests services while visiting a foreign domain. Concerned about security and privacy, the user would prefer to remain anonymous with respect to the foreign domain. That is, only the home domain authority should be informed as to the mobile user’s real identity, itinerary, whereabouts, etc. Another important issue, namely cloning phones, raises a number of concerns to many telecom carriers. Indeed, many telecommunication companies are losing money due to the use of clones or genuine mobile phones by impostors. One might argue that although it is rather easy to clone an AMPS phone, it is much trickier to clone a D-AMPS, a GSM, or an IS-95 phone. However, the security issue remains, and needs to be resolved in the next wireless network generation. Consequently, there has been a great deal of interest recently in designing mobile phones using new technologies, such as Boot Block flash technology used by Intel Corporation, that will make it much more difficult to clone cellular phones. However, to the best of my knowledge there is very little work being done at the software level. To combat cloning, cellular operators analyze usage to check for unusual patterns. Most obviously, they know that genuine phone cannot be in two places at once. If a phone is making more than one call at a time, it has definitely been cloned. Furthermore, to verify if a call is out of the client patterns, current software (i) does not have an efficient automatic process to warn clients about the impostors using their mobile phones; in most of these systems, human staff are used to do that (only lists of large bills are reviewed to identify cloned phones); (ii) has no efficient ways to control/identify impostors; and (iii) uses an “experimental satisfaction” to prove the correctness of the security framework. Some systems provide the billing process via the Web. However, the identification of a cloned phone is done only at the end of the month. This, unfortunately, is not quite efficient and may lead to a big loss of revenue for the carrier. The wireless Web opens up many new business opportunities, the most important of which use location-based technology. Ever since the mobile Internet was first suggested, antivirus companies have warned that viruses could attack cellular phones and PDSs. Timofonica was among the first viruses that attacked cell phones. Timofonica was an ordinary virus programmed to send abusive messages to random users of Spanish Telefonica mobile systems. Viruses are a threat to any computing platform and may be a threat to wireless terminals that include processing and memory akin to those of modern computers.

VI. RESULT AND DISCUSSION NETWORK SECURITY MANAGEMENT PLAN

An adequate security system management policy has long been an important issue. A comprehensive network security plan must also consider losses of privacy when we define authentication and authorization as well as losses of performance when we define key management and security protocols. Therefore, a security plan must encompass all of the elements that make up the wireless and/or wired network, and provide important services such as:

1. Access control, i.e., authorization by capability list, wrappers, and firewalls (access control matrix)
2. Confidentiality, i.e., we must ensure that information and transmitted messages are accessible only for reading by authorized parties
3. Authentication, i.e., the receiver must be able to confirm that the message is indeed from the right sender
4. Nonrepudiation, i.e., the sender cannot deny that the message was indeed sent by him/her
5. Integrity, i.e., the message has not been modified in transit
6. Availability, i.e., making sure that the system is available to authorized parties when needed
7. Security administration, i.e., checking audit trails, encryption and password management, maintenance of security equipment and services, and informing users of their responsibilities.

VII. INTRUSION DETECTION SYSTEMS (IDS)

Intrusion is most probably one of the key issues that wireless and mobile systems will have to deal with. The nature of wireless networks makes them very vulnerable to an adversary's malicious attacks. Generally speaking, an intrusion can be defined as an act of a person or proxy attempting to break into or misuse your system in violation of an established policy. Very little research work dealing with the intrusion problem has been done for wireless networks.

Generally speaking, intrusion can be classified as: (i) misuse intrusions, i.e., well-defined attacks against known system vulnerabilities; and (ii) anomaly intrusions, i.e., activities based on deviation from normal system usage patterns. Intrusion detection systems (IDS) are one of the latest security tools in the battle against these attacks. As is well known, it is very difficult to determine exactly which activities provide the best indicators for the established (normal) usage patterns. Thus, researchers have turned to using expert systems or knowledge-based intrusion detection to search for activities known to be indicative of possible intrusive behavior . The motivation behind this approach is to seek a proper behavior as opposed to a normal one. Knowledge-based intrusion detection schemes apply the knowledge they have accumulated about specific attacks and system vulnerabilities. Using this knowledge database, any action that is not explicitly recognized as an attack is considered acceptable. Otherwise, an alarm is triggered by the system.

There are many different intrusion systems available in the marketplace. Expert systems are based on knowledge-based intrusion detection techniques. Each attack is identified by a set of rules. Rule-based languages are used for modeling the knowledge that experts have accumulated about attacks/frauds. Information regarding some intruders has also been added to these systems. A major drawback of knowledge-based intrusion systems is the difficulty of gathering the information on the known attacks (which should be updated regularly) and developing a comprehensive set of rules that can be used to identify intrusive behaviors. Some systems use a combination of several approaches to cover both the normal and proper behaviorschemes . We refer to them as behavior-based intrusion detection. Their basic characteristic is that any action that does not match with a previously learned behavior triggers an alarm. The action is considered as intrusive. The main advantages of these systems are that they can exploit new and unforeseen attacks, and contribute to automatically discovering new attacks. However, their high false alarm rate is generally cited as a main drawback of these systems, due basically to the accuracy of the behavior information accumulated during the learning process.

VIII. SECURING DATA TRANSFER IN DIGITAL MOBILE SYSTEMS

All digital mobile systems provide security through some kind of encryption. Data can be encrypted in many ways, but algorithms used for secure data transfer fall into two categories: symmetric and asymmetric. Both rely on performing mathematical operations using a secret number known as a key. The difficulty with symmetric algorithms is that both parties need to have a copy of the key. On the other hand, asymmetric techniques use two separate keys for encryption and decryption. Usually, the encryption key can be publicly distributed, whereas the decryption key is held securely by the recipient.

The most widely used symmetric algorithm in DES (data encryption standard), developed by IBM in 1977. It uses a 56-bit key, which seemed unbreakable at that time. In 1997, a group of Internet users managed to read a DES-coded message. Most organization now use triple-DES, which uses 112 bits. The basic idea is that larger keys mean more possible permutations, and so better encryption. GMS encrypts all data between the phone and the base station using a code called A5 (The A stands for algorithm). The details of the code are kept secret to make it harder to crack. Unfortunately, details have been leaked out over the years and have been posted on hackers' web sites. Thus, we believe there is still much work to be done in the cloning mobile phone area. Several different asymmetric algorithms have been developed, each using a different type of "one-way" mathematical function. Rivest et al. proposed an efficient algorithm, which they refer to as RSA, that relies on the fact that factorization is more difficult than multiplication. Indeed, multiplying two prime numbers together is easy for a computer, but recovering those two numbers from the product is not. The main drawback of asymmetric schemes is that they use a lot of CPU, and so cannot be used to encrypt an entire message through a mobile phone. Instead, A5 encrypts the message itself using a symmetric algorithm, with a key randomly generated by the network and sent to the handset using an asymmetric algorithm.

IX. SECURING WIRELESS AD HOC NETWORKS

Many WLANs in use today need an infrastructure network. Infrastructure networks not only provide access to other networks, but also include forwarding functions, medium access control, etc. In these infrastructure-based wireless networks, communication typically takes place only between the wireless nodes and the access point, but not directly between the wireless nodes. Ad hoc wireless networks, however, do not need any infrastructure to work. Each node can communicate with another node; no access point controlling medium access is necessary. Mobile nodes within each other's radio range communicate directly via wireless links, whereas those that are far apart rely on other nodes to relay messages as routers. Node mobility in an ad hoc network causes frequent changes of the network topology.

Since an ad hoc network can be deployed rapidly at relatively low cost, it becomes an attractive option for commercial uses such as sensor networks or virtual classrooms. However, before an ad hoc network becomes a commodity, several security issues must first be resolved. On one hand, the security-sensitive applications of ad hoc networks require a high degree of security; on the other hand, ad hoc networks are inherently vulnerable to security attacks. Therefore, security mechanisms are indispensable for ad hoc networks.

As in any wireless or wired network, traffic across an ad hoc network can be highly vulnerable to security threats. Thus, to secure an ad hoc network, one should consider., availability, confidentiality, integrity, authentication, and nonrepudiation. but also new types of threats that are extended even to the basic structure of the networks. The salient characteristics of ad hoc networks pose both challenges and opportunities in achieving these security goals. Since ad hoc networks use wireless links, they are susceptible to link attacks ranging from passive eavesdropping to active impersonation, message replay, and message distortion. Active attacks might allow the adversary to delete messages, inject erroneous, modify messages, and impersonate a node, thereby violating availability, integrity, authentication, and Nonrepudiation.

(i) Intrusion Detection in Wireless Ad Hoc Networks

Most of the IDS systems developed for wired networks described in previous section cannot be applied to wireless networks. This is mainly due to the fact that today's network based IDSs, which rely on real-time traffic analysis, can no longer function in the wireless and mobile environments such wireless ad hoc networks. When compared with wired networks, in which traffic monitoring is usually done at switches, routers, and gateways, a wireless ad hoc network does not have traffic concentration points at which IDS can collect audit data for the entire network. Recall that in a wireless ad hoc network, each node can communicate with another node, and no access point controlling medium access is necessary. Mobile nodes within each other's radio range communicate directly via wireless links, whereas those that are far apart rely on other nodes to relay messages as routers.

Recently, Zhang and Lee examined the vulnerability of a wireless ad hoc network. They described an intrusion detection and response mechanism. In their approach, each node is responsible for detecting signs for intrusion locally and independently, but neighboring nodes can collaboratively investigate in a broader range. Individual IDS agents are placed on each and every node. Each IDS agent runs independently and monitors local activities such as user/system activities, communication activities, etc. These IDS agents collectively form the IDS system to protect the wireless ad hoc network against malicious attacks. If an IDS agent detects an intrusion from local data, neighboring IDS agents will collaborate in the global intrusion detection actions. Intrusion detection responses are provided by both the local response initiated by the IDS agent, and global response modules. The type of intrusion response depends on the type of network protocols and applications, and confidence (or certainty) in evidence. For example, the IDS agent can send a "reauthentication" request to all nodes in the network to prompt the end users to authenticate themselves (end hence their wireless nodes), using out-of-bound mechanisms (e,g., visual contacts). Only the reauthenticated nodes may collectively negotiate new communication channels, which in turn recognize each other as legitimate. Thus, the compromised and/or malicious nodes can be excluded. Last but not least, the authors use a secure communication module in their IDS system and provide a high-confidence communication channel among IDS agents. However, this work is still at an early stage, and no experimental data were provided to study the effectiveness of their scheme.

(ii) Securing Routing Protocol in Wireless Ad Hoc Networks

Security for any routing protocol is a very difficult problem to deal with. One can take advantage of the redundancies in the network topology, i.e., multiple routes between nodes, to achieve availability. The security of routing protocols is closely tied to the proper distribution of some keys that allow the creation of unforgeable credentials. Thus, designing secure key distribution in ad hoc networks is a challenging problem. Diffie–Hellman key exchange may indeed help to establish some temporary security between particular endpoints. However, they are also vulnerable to the man-in-the-middle attacks that are hard to defeat in an ad hoc network.

Recently, Zhang and Lee defined trace data to describe, for each node, the normal (i.e., legitimate) updates of routing information. Since a legitimate change in the route table can basically be caused by the physical movement(s) of node(s) or network membership changes, and each mobile node should use only reliable information that it can trust, the authors have decided to use data on a node's physical movements and the corresponding change in its routing table as the basis of the trace data. A normal profile on the trace data in effect specifies the correlation of physical movements of the nodes and the changes in the routing table. A classification algorithm is used to compute the classifier and to describe the changes measured by the percentage of changed routes and the percentage of changes in the sum of hops of all routes. A detection model that uses deviation scores distinguishes abnormal from normal updating of the routing table. Unfortunately, no experimental data was provided to study the performance and effectiveness of their scheme.

Public key protocols and symmetric key methods are also devilishly difficult, and without an infrastructure it is very hard to conceive of the use of certificate-based protocols. Multicast data distribution in ad hoc networks poses new types of security problems. Indeed, one should not forget that there will always be many different trust relationships that are hard to maintain between neighbours in a large community. Quality of service (QoS) control could be used to provide a reasonable solution to the multicast data distribution in ad hoc networks.

X. CONCLUSION

Flexibility and mobility makes Wireless Network provide all the functionality of wired network, but without the physical constraints of the wire itself. Wireless configurations include independent networks, suitable infrastructure networks, offering fully distributed data connectivity via microcells and roaming. In addition to offering end-user mobility within a networked environment, wirelessenables portable networks, allowing network to move with the knowledge workers that need them.

A wide range of wireless products are now available. By evaluating the strengths and differences of each of these offerings, knowledge network managers and users can choose a wireless solution that best meets their business and application objectives.

REFERENCES

[1.] D. S. Alexander, W. A. Arbaugh, A. D. Keromytis, and J. M. Smith, Safety and security of programmable networks infrastructures, IEEE Communications Magazine, 36, 10, 84–92.

[2.] A. Aziz and W. Diffie, Privacy and authentication for wireless local area networks, IEEE Pers.Comm., 1, 1, 25–31, 1994.

[3.] V. Bharghavan, Secure Wireless LANs, in Proceedings ACM Conference on Computer and Communications Security, 1994, pp. 10–17.

[4.] A. Boukerche and M. S. M. A. Notare, Neural fraud detection in mobile phone operations, 4thIEEE BioSP3, Bio-Inspired Solutions to Parallel Processing, May 2000, pp. 636–644.

[5.] A. Boukerche, M. SechiMoretti, and A. Notare, Applications of neural networks to mobile and wireless networks, In Biologically Inspired Solutions to Parallel and Distributed Computing, A.Zomaya (Ed.), New York: Wiley, 2001.

[6.] E. Brinksma. IS 8807—LOTOS—Language of Temporal Ordering Specifications, 1988.

[7.] D. Brown, M. Abadi, and R. M. Needham, A logic of authentication, ACM Transactions on Computer Systems, 8, 1, 18–36, 1995.

[8.] H. Demuth and M. Beale, Neural network tollbox—For use with MatLab, Matlab User's Guide,Version 3, pp. 7.1 – 7.33, 1998.

[9.] D. Denning, An intrusion-detection model, IEEE Transactions on Software Eng., 2(13),

[10.] 222–232, 1987.

[11.] 10. Y. Frankel, A. Herzberg, P. A. Karger, C. A. Kunzinger, and M. Yung, Security issues in a CDPD wireless network, IEEE Pers. Comm., 2, 4, 16–27, 1995.

[12.] H. Garavel, CADP/Eucalyptus Manual, INRIA, Grenoble, France, 1996.

[13.] V. Gupta and G. Montenegro, Secure and mobile networking, ACM/Baltzer MONET, 3,

[14.] 381–390, 1999.

[15.] N. Habra et al., Asax: Software architecture and rule-based language for universal audit trail analysis, in Proceedings 2nd European Symposium on Research in Computer Security, LNCS,vol. 648, 1992.

[16.] **322** SECURITY AND FRAUD DETECTION IN MOBILE AND WIRELESS NETWORKS

[17.] S. Jacob and M. S. Corsen, MANET Authentication architecture, MANET Internet Draft, Feb 1999.

[18.] J. Liu and L. Harn, Authentication of mobile users in personal communication systems, IEEE Symposium on Personnel Indoor and Mobile Radio Communication, 1996, pp. 1239–1242.

[19.] T. Lunt et al., Knowledge-Based Intrusion Detection, in Proceedings AI Systems in Government Conference, 1986.

[20.] T. Lunt, Automated audit trail analysis and intrusion detection: A survey, in Proceedings 11thInternational Computer Security Conference, 1988, pp. 65–73.

[21.] 18. S. Mohan, Privacy and authentication protocol for PCS, IEEE Personnel Communication, 1996, pp. 34–38.